SECTION X. KEYING MATERIAL MANAGEMENT

79. General. This section is applicable to those contractors who purchase CCI equipment and it only addresses what is termed “hard copy” key, i.e., physical keying material such as printed key lists, punched key tapes, punched key cards, etc. “Soft key” in electronic form is often employed in newer cryptographic equipments for key updating and similar functions, and is addressed in the operating instructions for the particular equipment.

80. Keying Material Source. Keying material for CCI equipment is produced by, and provided by the Government. When CCI equipment is acquired, it is used to protect information in a communications net which, from a cryptographic point of view, is known as a "cryptonet." CCI equipments operating in a single cryptonet must have compatible keying material to be able to correctly encrypt and decrypt communications. In order to manage the establishment of a cryptonet, and to ensure the provision of the correct keying materials to the proper members of the cryptonet, one party associated with the cryptonet is designated as the “Controlling Authority.”

81. Designation of the Controlling Authority. Controlling authorities should be designated primarily on the basis of their ability to perform their responsibilities. A controlling authority must be a member of the cryptonet and have some seniority or authority over the other members of the cryptonet. A controlling authority must have a means of communicating with cryptonet members (preferably multiple means) and with interested parties who may not be members of the cryptonet (e.g., Government contracting officers), and must be in a position to monitor the status of the cryptonet, i.e., to identify problems, or receive adequate information about net problems. The contractor who purchases the cryptographic equipment may work with the vendor, his Government contracting officer(s), or with the NSA (Y1) in proposing a controlling authority for the new cryptonet. The following guidance for the designation of a controlling authority is provided:

a. If there is a single Government Contracting Office involved, or if there is an identifiable lead Service/Department/Agency, the Contracting Officer, following his Department or Agency’s procedures, may designate who the controlling authority will be.

b. If there are multiple Government Contracting Offices involved with no identifiable lead service, then the contractor will coordinate with each of them and propose a controlling authority designation to NSA (Y1).

c. It is the purchasing contractor’s responsibility to ensure that a controlling authority designation proposal is made to NSA (Y1) early in the process of establishing a cryptonet, as this is the first step in obtaining the keying material necessary for cryptonet operation. The proposal can be developed by the leading Government Contracting Officer, by the purchasing contractor, or by the vendor, but it remains the responsibility of the purchasing contractor to ensure that the proposal is made to NSA (Y1).

d. All proposed designations of controlling authorities are subject to review by NSA (Y1).

For existing cryptonets which are significantly modified or expanded by the addition of new members, the current controlling authority must revalidate his role. This should be accomplished through existing Department and Agency regulations and procedures, if applicable, or directly to NSA (Y1). Although in most cases the designation of the controlling authority will not change, there may be some net membership changes for which redesignation of the controlling authority becomes practical. If there is any difficulty, confusion, or dispute involved in the selection of a controlling authority, and it cannot be resolved in coordination with the lead Government Agency, the problem should be referred to NSA (Y1).

82. Responsibilities of the Controlling Authority. The controlling authority for a cryptonet has responsibilities which fall into three broad categories: cryptonet management, logistics, and security. The responsibilities of the controlling authority include:

a. Cryptonet Management:

(1) Establishing a cryptonet by designating cryptonet members.

(2) Specifying the status of the keying material, to include the date on which the first edition will become effective, the effective dates for remaining material; and keeping all cryptonet members informed of this information. (NOTE: For classified keying material, the effective dates are classified CONFIDENTIAL.)

(3) Specifying the key change time for the cryptonet.

(4) Authorizing local reproduction of copies of keying material controlled by the controlling authority in situations where established cryptologistic channels cannot supply the material in time to meet urgent, unprogrammed, operational requirements; and ensuring that the reproduced material is properly controlled and destroyed in the same manner as the original material.

(5) Reporting to NSA (Y1 and S042) incidents of faulty keying material or the unauthorized transmission of keying information.

(6) Ensuring that COMSEC insecurity reporting instructions are disseminated to all cryptonet members (with special emphasis on how and where to send insecurity reports to the controlling authority).

(7) Ensuring that prescribed allowances of on-hand keying materials at cryptonet member locations are adequate for potential emergency supersessions.

(8) Conducting annual reviews to confirm that there is a continuing requirement for the cryptonet keying material, including the quantity, quality, and operational effectiveness of that material. This review will normally be conducted as an annual update of the Keying material Support Plan (KMSP) described in paragraph 84.

b. Logistics:

(1) Notifying NSA (Y1) of any changes in the membership of the cryptonet and of any changes in the quantity of material each member is to receive.

(2) Notifying NSA (Y1) of any changes in the effective dates and key change times of cryptonet keying material.

c. Security (see also Section XVI, COMSEC Insecurity Reporting Requirements):

(1) Evaluating the security impact of reports of physical insecurities of superseded, effective, and future cryptonet keying materials; and making a determination as to whether or not a compromise of the material has occurred.

(2) Notifying appropriate Government authorities, cryptonet members, and NSA (S21) of the results of the evaluation.

(3) Directing emergency supersession of keying material; taking other appropriate actions in response to actual or suspected compromises (see Appendix 1 this Supplement).

(4) Ensuring that NSA (S21) and other appropriate Government authorities are notified of all incidents of suspected theft, subversion, espionage, defection, tampering, or sabotage affecting COMSEC materials.

(5) Directing emergency extensions of keying material cryptoperiods up to 24 hours (unless the specific cryptosystem doctrine prohibits such an extension or authorizes a longer period), and notifying NSA (S21) of this action.

83. Considerations in Establishing a Cryptonet. To fulfill its prescribed duties effectively, the controlling authority requires accurate information on all aspects of the cryptonet, and must have the capability to communicate with all cryptonet members. In particular, the controlling authority should be familiar with all aspects of the handling of keying material in his cryptonet, and with the most expeditious ways of promulgating supersession and other emergency information to all holders of the keying material. Some of the specific items to consider in establishing a cryptonet include the following:

a. The effective key change times should be as convenient as possible for all members of the cryptonet. A knowledge of the net operations at member locations, across different time zones, is helpful in picking an optimum key change time.

b. For security reasons, cryptonet size should be kept as small as possible. A goal should be to limit the number of people who have access to the key to the absolute minimum.

c. The date and time of key changes must be uniform throughout the cryptonet.

d. Cryptologistics should be carefully considered. How will the keying material get to each member of the cryptonet? Should new COMSEC accounts or subaccounts be established? Should existing accounts be closed down?

e. The availability of information for the controlling authority, and how it will reach the controlling authority are important points. In order to properly perform, the controlling authority must know the current status of the cryptonet.

f. Operational interoperability requirements may dictate cryptographic netting and subnetting schemes.

g. The quantity, sensitivity and classification (if applicable) of the information to be transmitted over the cryptonet must be considered in the determination of the classification of the keying material.

84. Keying Material Support Plan (KMSP). A primary responsibility of the controlling authority is the preparation of the "Keying Material Support Plan" or KMSP, which establishes how keying material will be provided to the cryptonet during its operational lifetime. Authorized vendors are required under their Memorandum of Agreement with NSA to offer assistance in the preparation of the KMSP, although the controlling authority may elect to prepare the KMSP unassisted, or-use the COMSEC vendor's or the Government's assistance through the lead Contracting Officer.

If a Government entity is the controlling authority, it will prepare the KMSP in accordance with its department or agency procedures. The KMSP should be filed with NSA (Y1) to allow adequate lead time for the production and distribution of the right amounts of keying material. For planning purposes, a minimum of 120 days is required from the time NSA receives an order for keying material until it is produced and shipped from NSA. The KMSP will be submitted to NSA (Y1) for review and approval as follows:

a. If a contractor is the controlling authority and there is a lead service, department, or agency, the contractor will submit the KMSP through its appropriate contracting officer, who will forward the KMSP via department or agency channels or, if appropriate, directly to NSA (Y1).

b. If a Government entity is the controlling authority, it will submit the KMSP in accordance with department or agency procedures, and forward it to NSA (Y1).

c. If a contractor is the controlling authority and there is no lead service, department or agency, it will submit the KMSP directly to NSA (Y1).

85. Contents of the Keying material Support Plan. The KMSP must contain adequately detailed information about the cryptonet so that NSA can produce and provide the correct types and amounts of keying materials to the right place at the right time. There must also be enough information so that NSA can ensure that security concerns are addressed, e.g. , making sure that no SECRET keying material is sent to an account authorized to hold only CONFIDENTIAL materials. The following are the specific topics which must be addressed in a KMSP:

a. The Operational Need: Brief statement of the need for the cryptonet, i.e., the Government contracts and types of information involved. Specify classification and/or sensitivity of the information.

b. The Operational Concept: Statement on the operational structure of the net; days/times of operation; identification of net control and alternates, as well as subletting.

c. Controlling Authority: Identifying the cryptonet controlling authority, including names of points-of-contact, complete address information, and telephone numbers.

d. Contracting Office(s): Identity of the Government contracting office or offices served by or associated with the cryptonet; names, addresses and telephone numbers of contracting officers.

e. Keying Material Specification: The following information on the keying material which is needed for the operation of the cryptonet:

(1) Identity of cryptographic equipment (and fill devices) which will use the keying material.

(2) Use of keying material: operational; maintenance; training.

(3) Quantity required (copy counts). Also identify editions if there are special circumstances.

(4) Date required initial operational capability.

(5) Classification (or specify UNCLASSIFIED).

f. The Distribution Plan: Description of the keying materials to be shipped, identifying the originator (normally NSA) and the receiver. A block diagram of the shipping paths from NSA to the material's final destination should be included (it need only address the major points of accounting transfers). It must provide complete COMSEC account information for all major modes in the distribution plan. The distribution plan must identify any primary COMSEC accounts which will receive materials in bulk shipments from NSA, and identify any subaccounts which will not be serviced by their primary accounts. The distribution plan must also address how the keying materials will be distributed from the COMSEC accounts to the actual users.

g. Other Information: Any additional information which the controlling authority feels is significant, or is unique to his particular cryptonet or keying material.

86. Annual Reviews of Keying Material. The controlling authority is required to review the adequacy and currency of the KMSP annually, and provide any changes in writing to NSA (Y1) no later than 1 July of each year. Written negative reports (i.e., the review indicates that no changes are necessary to the current KMSP) are required. Particular points to be addressed in the annual KMSP review include the following:

a. Changes in cryptonet membership.

b. Changes in addresses, names of contacts, and telephone numbers.

c. Changes in the classification or sensitivity of the information being communicated on the net.

d. Any changes in the quantity of materials distributed. Controlling authorities must ensure that COMSEC accounts have enough material on hand for regular and emergency supersessions, but not too much material (which negatively affects security, storage, bookkeeping, etc.).

(1) User COMSEC account inventories should generally not exceed four months' total supply of monthly superseded material, including effective material.

(2) A minimum of one back-up edition of keying material must be held at the user COMSEC account regardless of the normal cryptoperiod length.

e. Any planned changes or cancellations of requirements.